

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-331449

(P2001-331449A)

(43) 公開日 平成13年11月30日 (2001. 11. 30)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マコ-ト*(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B
	12/14		3 2 0 A
H 0 4 L 9/32	3 2 0	H 0 4 L 9/00	6 7 3 C
			6 7 5 A

審査請求 有 請求項の数20 O L (全 10 頁)

(21) 出願番号 特願2001-61999(P2001-61999)

(22) 出願日 平成13年3月6日(2001. 3. 6)

(31) 優先権主張番号 特願2000-69079(P2000-69079)

(32) 優先日 平成12年3月13日(2000. 3. 13)

(33) 優先権主張国 日本 (J P)

(71) 出願人 500257300  
ヤフー株式会社  
東京都港区北青山3-6-7

(72) 発明者 楠 正憲  
東京都世田谷区千歳台1-21-1 ジェ  
ー・ステージ千歳台101号室

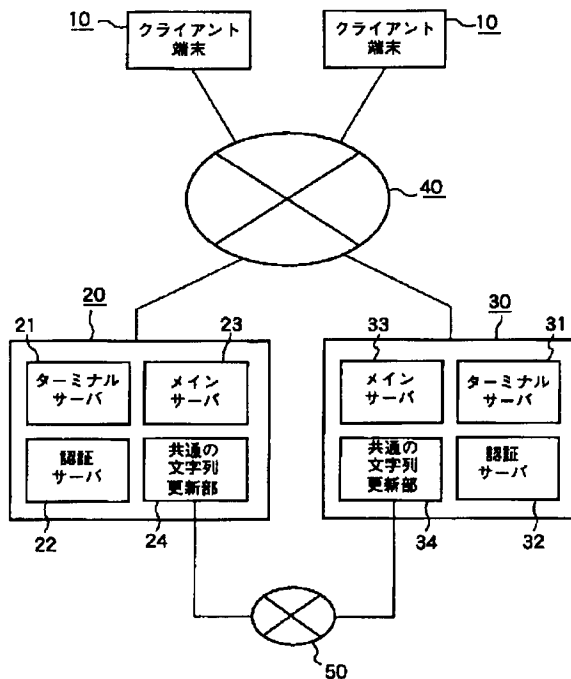
(74) 代理人 100058479  
弁理士 鈴江 武彦 (外5名)

(54) 【発明の名称】 アクセス認証システム、記憶媒体、プログラム及びアクセス認証方法

(57) 【要約】

【課題】 1つのサーバに対しての個人情報に基づいて、各種サービスを提供する他のサーバを利用可能とするアクセス認証システムを提供すること。

【解決手段】 クライアント端末10から入力された個別情報に基づいて第1のターミナルサーバへの接続の可否を認証するとともに、クライアントパラメータPを符号化した第1のチケットデータを作成し、第2のターミナルサーバに転送する第1の認証サーバ22と、クライアントパラメータPの正当性及び第1のチケットデータD1の行使の有無を検証するとともに、クライアントパラメータPを符号化した第2のチケットデータD2を作成し、第2のチケットデータD2と第1のチケットデータD1とを照合し、第2のターミナルサーバ31へクライアント端末10の接続可否を指示する第2の認証サーバ32とを備えている。



## 【特許請求の範囲】

【請求項1】第1のターミナルサーバを経由してクライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記第1のターミナルサーバに対して上記クライアントから入力された個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成し、上記第2のターミナルサーバに転送する第1の認証サーバと、  
上記クライアントパラメータの正当性及び上記第1のチケットデータの行使の有無を検証するとともに、上記クライアントパラメータを所定の規則で符号化した第2のチケットデータを作成し、この第2のチケットデータと上記第1のチケットデータとを照合し、上記第2のターミナルサーバへ上記クライアントの接続可否を指示する第2の認証サーバとを備えていることを特徴とするアクセス認証システム。

【請求項2】上記所定の規則は、一方向関数による要約であることを特徴とする請求項1に記載のアクセス認証システム。

【請求項3】上記クライアントパラメータには、上記クライアントのID、アクセス元IPアドレス、上記第1のチケットデータの有効期限のうち少なくとも1つが含まれていることを特徴とする請求項1に記載のアクセス認証システム。

【請求項4】上記第1及び第2の認証サーバにおいて、上記第1及び第2のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする請求項1に記載のアクセス認証システム。

【請求項5】上記共通の文字列は、所定のタイミングで変更されるものであることを特徴とする請求項4に記載のアクセス認証システム。

【請求項6】第1のターミナルサーバを経由してクライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記第1のターミナルサーバに対して上記クライアントから入力されたID及びパスワードに基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記ID、上記クライアントのアクセス元IPアドレス、所定の有効期限、共通の文字列からなるクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成し、上記第2のターミナルサーバに転送する第1の認証サーバと、  
上記第2のターミナルサーバに対して上記クライアントから入力されたアクセス元IPアドレスと上記クライアントパラメータのアクセス元IPアドレスとを照合し、上記有効期限内のアクセスであるか否かを判断し、上記第1のチケットデータの行使の有無を判断し、上記クラ

アントパラメータを上記所定の規則で符号化した第2のチケットデータを作成し、この第2のチケットデータと上記第1のチケットデータとを照合することで、上記第2のターミナルサーバへ上記クライアントの接続可否を指示する第2の認証サーバとを備えていることを特徴とするアクセス認証システム。

【請求項7】第1のターミナルサーバを経由してクライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

10 上記第1のターミナルサーバにおいて上記クライアントから入力された個別情報を取得する第1の個別情報取得手段と、

上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証する第1の認証手段と、

上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成する第1のチケットデータ作成手段と、

上記第2のターミナルサーバに転送する転送手段と、

20 上記第2のターミナルサーバにおいて上記クライアントから入力された個別情報を取得する第2の個別情報取得手段と、

上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第2のチケットデータを作成し、この第2のチケットデータと上記第1のチケットデータとを照合し、上記第2のターミナルサーバへ上記クライアントの接続可否を認証する第2の認証手段とを備えていることを特徴とするアクセス認証システム。

30 【請求項8】上記所定の規則は、一方向関数による要約であることを特徴とする請求項7に記載のアクセス認証システム。

【請求項9】上記第1及び第2のチケットデータ作成手段は、上記第1及び第2のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする請求項7に記載のアクセス認証システム。

【請求項10】上記第2の認証手段は、上記第1のチケットデータの有効性を判断することを特徴とする請求項7に記載のアクセス認証システム。

40 【請求項11】上記第2の認証手段は、上記クライアントパラメータの正当性を判断することを含むことを特徴とする請求項7に記載のアクセス認証システム。

【請求項12】第1のターミナルサーバを経由してクライアントに接続サービスを行うアクセス認証システムにおいて、

上記クライアントから個別情報を取得する第1の個別情報取得手段と、

上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証する第1認証手段と、

50 この第1認証手段にて認証が可とされた場合に、少なく

とも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成する第1のチケットデータ作成手段と、

上記第1のチケットデータを転送する転送手段とを備えていることを特徴とするアクセス認証システム。

【請求項13】クライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、

上記クライアントの個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを取得する第1のチケットデータ取得手段と、  
上記クライアントから個別情報を取得する第2の個別情報取得手段と、

この第2の個別情報取得手段にて取得された個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成する第2のチケットデータ作成手段と、

上記第2のチケットデータと上記第1のチケットデータとを照合し、上記第2のターミナルサーバへ上記クライアントの接続可否を判断する判断手段とを備えていることを特徴とするアクセス認証システム。

【請求項14】コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、

第1のターミナルサーバにおいてクライアントから個別情報を取得させる第1の個別情報取得手段と、

上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証させる第1認証手段と、

上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成させる第1のチケットデータ作成手段と、

上記第1のチケットデータを第2のターミナルサーバに転送させる転送手段と、

上記第2のターミナルサーバにおいて上記第1のチケットデータを取得させる第1のチケットデータ取得手段と、

上記第2のターミナルサーバにおいて上記クライアントから個別情報を取得させる第2の個別情報取得手段と、  
上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成させる第2のチケットデータ作成手段と、

上記第1のチケットデータと上記第2のチケットデータとを照合し、上記第2のターミナルサーバへの上記クライアントの接続可否を認証させる第2認証手段とを備えていることを特徴とする記憶媒体。

【請求項15】コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、

第1のターミナルサーバにおいてクライアントから個別情報を取得させる第1の個別情報取得手段と、

上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証させる第1認証手段と、

上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成させる第1のチケットデータ作成手段と、

10 上記第1のチケットデータを転送させる転送手段とを備えていることを特徴とする記憶媒体。

【請求項16】コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、

第2のターミナルサーバにおいて上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した上記第1のチケットデータを取得させる第1のチケットデータ取得手段と、

20 上記第2のターミナルサーバにおいて上記クライアントから個別情報を取得させる第2の個別情報取得手段と、  
上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成させる第2のチケットデータ作成手段と、

上記第1のチケットデータと上記第2のチケットデータとを照合し、上記第2のターミナルサーバへの上記クライアントの接続可否を認証させる第2認証手段とを備えていることを特徴とする記憶媒体。

【請求項17】コンピュータを動作させるためのプログラムにおいて、

30 第1のターミナルサーバにおいてクライアントから個別情報を取得させる第1の個別情報取得手段と、  
上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証させる第1認証手段と、

上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成させる第1のチケットデータ作成手段と、

40 上記第1のチケットデータを第2のターミナルサーバに転送させる転送手段と、  
上記第2のターミナルサーバにおいて上記第1のチケットデータを取得させる第1のチケットデータ取得手段と、

上記第2のターミナルサーバにおいて上記クライアントから個別情報を取得させる第2の個別情報取得手段と、  
上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成させる第2のチケットデータ作成手段と、

50 上記第1のチケットデータと上記第2のチケットデータとを照合し、上記第2のターミナルサーバへの上記クラ

クライアントの接続可否を認証させる第2認証手段とを備えていることを特徴とするプログラム。

【請求項18】コンピュータを動作させるためのプログラムにおいて、

第1のターミナルサーバにおいてクライアントから個別情報を取得させる第1の個別情報取得手段と、上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証させる第1認証手段と、

上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成させる第1のチケットデータ作成手段と、

上記第1のチケットデータを転送させる転送手段とを備えていることを特徴とするプログラム。

【請求項19】コンピュータを動作させるためのプログラムにおいて、

第2のターミナルサーバにおいてクライアントの個別情報の一部を含むクライアントパラメータを所定の規則で符号化した上記第1のチケットデータを取得させる第1のチケットデータ取得手段と、

上記第2のターミナルサーバにおいて上記クライアントから個別情報を取得させる第2の個別情報取得手段と、上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成させる第2のチケットデータ作成手段と、

上記第1のチケットデータと上記第2のチケットデータとを照合し、上記第2のターミナルサーバへの上記クライアントの接続可否を認証させる第2認証手段とを備えていることを特徴とするプログラム。

【請求項20】第1のターミナルサーバを経由してクライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証方法において、

上記第1のターミナルサーバへの上記クライアントの接続の可否を認証する第1の認証ステップと、

上記クライアントから入力された個別情報の少なくとも一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成する第1チケットデータ作成ステップと、

上記第2のターミナルサーバに上記クライアントパラメータ及び上記第1のチケットデータを転送するデータ転送ステップと、

上記第1のターミナルサーバにおける上記クライアントパラメータの正当性及び上記第1のチケットデータの行使の有無を検証する検証ステップと、

上記クライアントパラメータを所定の規則で符号化した第2のチケットデータを作成する第2チケットデータ作成ステップと、

この第2のチケットデータと上記第1のチケットデータとを照合するチケットデータ照合ステップと、

上記検証ステップ及び上記チケットデータ照合ステップにおける結果に基づいて、上記第2のターミナルサーバへ上記クライアントの接続可否を指示する第2の認証ステップとを備えていることを特徴とするアクセス認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、所定のアプリケーションプロバイダへのアクセス権を予め有するユーザが異なるアプリケーションプロバイダへのアクセス権を得るためのアクセス認証システム及びアクセス認証方法に関する。

【0002】

【従来の技術】ユーザはインターネットを介して様々な情報サービス等の各種サービスを提供するサービス提供者を利用することができる。サービス提供者とは、インターネットを介して接続されたクライアント端末に対してデータやコンテンツを提供したり、情報処理サービスを提供する業者を指している。サービス提供者はそれぞれ独立しており、ユーザは利用したいサービス提供者と契約し、それぞれIDとパスワードを持つことでアクセス権を得るようにしている。

【0003】

【発明が解決しようとする課題】しかし、サービス提供者は増えており、ユーザがそれぞれのサービス提供者と契約するのはIDやパスワードを管理する上で煩雑であった。また、各サービス提供者が提供できるサービスの種類には限界があった。

【0004】一方、一つのIDとパスワードを複数のサービス提供者間で共通化して用いる方法も考えられるが、ID及びパスワードの両方を各サービス提供者で保持することになるため、課金や秘密保持の点で問題があった。

【0005】そこで本発明は、1つのサーバ（サービス提供者）に対しての個人情報（ID及びパスワード）のみで、各種サービスを提供する他のサーバ（サービス提供者）を個人情報の全てを開示することなく利用することができるようにするためのアクセス認証システム、記憶媒体、プログラム及びアクセス認証方法を提供することを目的としている。

【0006】

【課題を解決するための手段】上記課題を解決し目的を達成するために、本発明のアクセス認証システム、記憶媒体、プログラム及びアクセス認証方法は次のように構成されている。

【0007】（1）第1のターミナルサーバを経由してクライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、上記第1のターミナルサーバに対して上記クライアントから入力された個別情報に基づいて上記第1のターミナルサーバへの

上記クライアントの接続の可否を認証するとともに、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成し、上記第2のターミナルサーバに転送する第1の認証サーバと、上記クライアントパラメータの正当性及び上記第1のチケットデータの行使の有無を検証するとともに、上記クライアントパラメータを所定の規則で符号化した第2のチケットデータを作成し、この第2のチケットデータと上記第1のチケットデータとを照合し、上記第2のターミナルサーバへ上記クライアントの接続可否を指示する第2の認証サーバとを備えていることを特徴とする。

【0008】(2) 上記(1)に記載されたアクセス認証システムであって、上記所定の規則は、一方向関数による要約であることを特徴とする。

【0009】(3) 上記(1)に記載されたアクセス認証システムであって、上記クライアントパラメータには、上記クライアントのID、アクセス元IPアドレス、上記第1のチケットデータの有効期限のうち少なくとも1つが含まれていることを特徴とする。

【0010】(4) 上記(1)に記載されたアクセス認証システムであって、上記第1及び第2の認証サーバにおいて、上記第1及び第2のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする。

【0011】(5) 上記(4)に記載されたアクセス認証システムであって、上記共通の文字列は、所定のタイミングで変更されるものであることを特徴とする。

【0012】(6) 第1のターミナルサーバを経由してクライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、上記第1のターミナルサーバに対して上記クライアントから入力されたID及びパスワードに基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証するとともに、上記ID、上記クライアントのアクセス元IPアドレス、所定の有効期限、共通の文字列からなるクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成し、上記第2のターミナルサーバに転送する第1の認証サーバと、上記第2のターミナルサーバに対して上記クライアントから入力されたアクセス元IPアドレスと上記クライアントパラメータのアクセス元IPアドレスとを照合し、上記有効期限内のアクセスであるか否かを判断し、上記第1のチケットデータの行使の有無を判断し、上記クライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成し、この第2のチケットデータと上記第1のチケットデータとを照合することで、上記第2のターミナルサーバへ上記クライアントの接続可否を指示する第2の認証サーバとを備えていることを特徴とする。

【0013】(7) 第1のターミナルサーバを経由して

クライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、上記第1のターミナルサーバにおいて上記クライアントから入力された個別情報を取得する第1の個別情報取得手段と、上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証する第1の認証手段と、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成する第1のチケットデータ作成手段と、上記第2のターミナルサーバにおいて上記クライアントから入力された個別情報を取得する第2の個別情報取得手段と、上記個人情報の一部を含むクライアントパラメータを所定の規則で符号化した第2のチケットデータを作成し、この第2のチケットデータと上記第1のチケットデータとを照合し、上記第2のターミナルサーバへ上記クライアントの接続可否を認証する第2の認証手段とを備えていることを特徴とする。

【0014】(8) 上記(7)に記載されたアクセス認証システムであって、上記所定の規則は、一方向関数による要約であることを特徴とする。

【0015】(9) 上記(7)に記載されたアクセス認証システムであって、上記第1及び第2のチケットデータ作成手段は、上記第1及び第2のチケットデータを作成する際に、予め定められた共通の文字列を含めることを特徴とする。

【0016】(10) 上記(7)に記載されたアクセス認証システムであって、上記第2の認証手段は、上記第1のチケットデータの有効性を判断することを特徴とする。

【0017】(11) 上記(7)に記載されたアクセス認証システムであって、上記第2の認証手段は、上記クライアントパラメータの正当性を判断することを含むことを特徴とする。

【0018】(12) 第1のターミナルサーバを経由してクライアントに接続サービスを行うアクセス認証システムにおいて、上記クライアントから個別情報を取得する第1の個別情報取得手段と、上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証する第1認証手段と、この第1認証手段にて認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成する第1のチケットデータ作成手段と、上記第1のチケットデータを転送する転送手段とを備えていることを特徴とする。

【0019】(13) クライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証システムにおいて、上記クライアントの個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを取得する第1のチケットデータ取得手段

と、上記クライアントから個別情報を取得する第2の個別情報取得手段と、この第2の個別情報取得手段にて取得された個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成する第2のチケットデータ作成手段と、上記第2のチケットデータと上記第1のチケットデータとを照合し、上記第2のターミナルサーバへ上記クライアントの接続可否を判断する判断手段とを備えていることを特徴とする。

【0020】(14) コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、第1のターミナルサーバにおいてクライアントから個別情報を取得させる第1の個別情報取得手段と、上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証させる第1認証手段と、上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成させる第1のチケットデータ作成手段と、上記第1のチケットデータを第2のターミナルサーバに転送させる転送手段と、上記第2のターミナルサーバにおいて上記第1のチケットデータを取得させる第1のチケットデータ取得手段と、上記第2のターミナルサーバにおいて上記クライアントから個別情報を取得させる第2の個別情報取得手段と、上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成させる第2のチケットデータ作成手段と、上記第1のチケットデータと上記第2のチケットデータとを照合し、上記第2のターミナルサーバへの上記クライアントの接続可否を認証させる第2認証手段とを備えていることを特徴とする。

【0021】(15) コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、第1のターミナルサーバにおいてクライアントから個別情報を取得させる第1の個別情報取得手段と、上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証させる第1認証手段と、上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成させる第1のチケットデータ作成手段と、上記第1のチケットデータを転送させる転送手段とを備えていることを特徴とする。

【0022】(16) コンピュータを動作させるためのプログラムを記憶したコンピュータ読取り可能な記憶媒体において、上記プログラムは、第2のターミナルサーバにおいて上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した上記第1のチケットデータを取得させる第1のチケットデータ取得手段と、上

記第2のターミナルサーバにおいて上記クライアントから個別情報を取得させる第2の個別情報取得手段と、上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成させる第2のチケットデータ作成手段と、上記第1のチケットデータと上記第2のチケットデータとを照合し、上記第2のターミナルサーバへの上記クライアントの接続可否を認証させる第2認証手段とを備えていることを特徴とする。

【0023】(17) コンピュータを動作させるためのプログラムにおいて、第1のターミナルサーバにおいてクライアントから個別情報を取得させる第1の個別情報取得手段と、上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証させる第1認証手段と、上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成させる第1のチケットデータ作成手段と、上記第1のチケットデータを第2のターミナルサーバに転送させる転送手段と、上記第2のターミナルサーバにおいて上記第1のチケットデータを取得させる第1のチケットデータ取得手段と、上記第2のターミナルサーバにおいて上記クライアントから個別情報を取得させる第2の個別情報取得手段と、上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成させる第2のチケットデータ作成手段と、上記第1のチケットデータと上記第2のチケットデータとを照合し、上記第2のターミナルサーバへの上記クライアントの接続可否を認証させる第2認証手段とを備えていることを特徴とする。

【0024】(18) コンピュータを動作させるためのプログラムにおいて、第1のターミナルサーバにおいてクライアントから個別情報を取得させる第1の個別情報取得手段と、上記個別情報に基づいて上記第1のターミナルサーバへの上記クライアントの接続の可否を認証させる第1認証手段と、上記クライアントの接続の認証が可とされた場合に、少なくとも上記個別情報の一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成させる第1のチケットデータ作成手段と、上記第1のチケットデータを転送させる転送手段とを備えていることを特徴とする。

【0025】(19) コンピュータを動作させるためのプログラムにおいて、第2のターミナルサーバにおいてクライアントの個別情報の一部を含むクライアントパラメータを所定の規則で符号化した上記第1のチケットデータを取得させる第1のチケットデータ取得手段と、上記第2のターミナルサーバにおいて上記クライアントから個別情報を取得させる第2の個別情報取得手段と、上記個別情報の一部を含むクライアントパラメータを上記所定の規則で符号化した第2のチケットデータを作成さ

せる第2のチケットデータ作成手段と、上記第1のチケットデータと上記第2のチケットデータとを照合し、上記第2のターミナルサーバへの上記クライアントの接続可否を認証させる第2認証手段とを備えていることを特徴とする。

【0026】(20)第1のターミナルサーバを經由してクライアントに第2のターミナルサーバへの接続サービスを行うアクセス認証方法において、上記第1のターミナルサーバへの上記クライアントの接続の可否を認証する第1の認証ステップと、上記クライアントから入力された個別情報の少なくとも一部を含むクライアントパラメータを所定の規則で符号化した第1のチケットデータを作成する第1チケットデータ作成ステップと、上記第2のターミナルサーバに上記クライアントパラメータ及び上記第1のチケットデータを転送するデータ転送ステップと、上記第1のターミナルサーバにおける上記クライアントパラメータの正当性及び上記第1のチケットデータの行使の有無を検証する検証ステップと、上記クライアントパラメータを所定の規則で符号化した第2のチケットデータを作成する第2チケットデータ作成ステップと、この第2のチケットデータと上記第1のチケットデータとを照合するチケットデータ照合ステップと、上記検証ステップ及び上記チケットデータ照合ステップにおける結果に基づいて、上記第2のターミナルサーバへ上記クライアントの接続可否を指示する第2の認証ステップとを備えていることを特徴とする。

【0027】

【発明の実施の形態】図1は本発明の一実施の形態に係るアクセス認証システムの構成を示す図、図2の

(a)、(b)は同アクセス認証システムに組み込まれた認証サーバ22、32の構成を示すブロック図、図3はアクセス認証の手順を示すフロー図である。なお、本実施の形態はソフトウェア処理により実現する場合も含まれる。

【0028】図1中10はユーザのクライアント端末、20はユーザと契約関係にあるサービス提供先サービス提供者、30はユーザと直接の契約関係のないサービス提供元サービス提供者、40はインターネット回線、50は電話回線を示している。

【0029】サービス提供先サービス提供者20は、インターネット回線40に接続されたターミナルサーバ(第1のターミナルサーバ)21と、このターミナルサーバ21に接続され後述するような認証等を行う認証サーバ(第1の認証サーバ)22と、ターミナルサーバ22に接続されるとともに情報サービスを提供するメインサーバ23と、電話回線50に接続された共通の文字列更新部24とを備えている。

【0030】認証サーバ22は、第1のターミナルサーバ21に対してクライアント端末10から入力されたID及びパスワードに基づいてターミナルサーバ21への

クライアント端末10からの接続の可否を認証する認証部22aと、クライアント端末10のアクセス元IPアドレスを検出するIPアドレス検出部22bと、後述する第1チケット(第1のチケットデータ)の有効期限を生成する有効期限生成部22cと、クライアントパラメータP、すなわちID、クライアントのアクセス元IPアドレス、有効期限生成部22cで生成された有効期限、共通の文字列更新部24で更新された最新の共通の文字列を一方向関数で要約する等の所定の規則を用いて第1チケットデータD1を作成するチケットデータ生成部22dと、クライアントパラメータP及び第1チケットデータを認証サーバ32にインターネット回線40及びターミナルサーバ31を介して転送する転送部22eとを備えている。

【0031】サービス提供元サービス提供者30は、インターネット回線40に接続されたターミナルサーバ(第2のターミナルサーバ)31と、このターミナルサーバ31に接続され後述するような認証等を行う認証サーバ(第2の認証サーバ)32と、ターミナルサーバ31に接続されるとともに情報サービスを提供するメインサーバ33と、電話回線50に接続された共通の文字列更新部34とを備えている。

【0032】認証サーバ32は、ターミナルサーバ31に対してクライアント端末10から入力されたアクセス元IPアドレスと上述した認証サーバ22から転送されたクライアントパラメータPのアクセス元IPアドレスとを照合するアクセス元IPアドレス照合部32aと、有効期限内のアクセスであるか否かを判断する有効期限判断部32bと、第1のチケットデータD1の行使の有無を判断するチケット行使判断部32cと、転送されたクライアントパラメータPを上述した規則と同一の規則で符号化した第2のチケットデータD2を作成するチケットデータ生成部32dと、第2のチケットデータD2と第1のチケットデータD1とを照合することで、第2のターミナルサーバ31へクライアント端末10からの接続可否を指示する認証部32eとを備えている。

【0033】共通の文字列更新部24及び共通の文字列更新部34は、文字列から構成される同一の共通の文字列を保持しており、定期的に更新されている。

【0034】このように構成されていると、ユーザがクライアント端末10からメインサーバ33にアクセスする場合には次のように行われる。すなわち、ユーザはクライアント端末10からインターネット回線40を介してターミナルサーバ21に接続を行う。このとき、ユーザはサービス提供先サービス提供者が提供するログイン画面に自己のID及びパスワードを入力する(ST10)。このとき、ターミナルサーバ21では、任意のアクセス制限を行い(ST11)、アクセスが禁止された場合にはログインが拒否される(ST12)。

【0035】ST2においてアクセスが許可された場合

には、ID、パスワード、アクセス元IPアドレスが認証サーバ22に送られ、認証部22aにてID及びパスワードに基づいてユーザ認証を行い(ST13)、認証に失敗した場合にはログインが拒否される(ST14)。なお、この時点でメインサーバ23へのアクセスが許可される。

【0036】ST4においてユーザ認証が成功した場合には、IPアドレス検出部22bにおいてクライアント端末10のアクセス元IPアドレスが検出され、有効期限生成部22cにおいて第1チケットデータD1の有効期限を生成する。そして、チケットデータ生成部22dにおいて、クライアントパラメータP(ID、アクセス元IPアドレス、有効期限、共通の文字列)を一方関数で要約して第1チケットデータD1を作成する(ST15)。

【0037】次に、転送部22eによりクライアントパラメータP及び第1チケットデータD1を認証サーバ32にインターネット回線40及びターミナルサーバ31を介して転送する(ST16)。

【0038】サービス提供元サービス提供者30の認証サーバ32では、アクセス元IPアドレス照合部32aによりアクセス元IPアドレス照合部32aターミナルサーバ31に対してクライアント端末10から入力されたアクセス元IPアドレスと上述した認証サーバ22から転送されたクライアントパラメータPのアクセス元IPアドレスとを照合し(ST20)、不一致である場合にはログインは拒否される(ST21)。

【0039】次に、有効期限判断部32bにより、有効期限内のアクセスであるか否かを判断し(ST22)、有効期限を経過している場合には無効とされログインは拒否される(ST23)。

【0040】次に、チケット行使判断部32cにより、第1のチケットデータD1の行使の有無を判断し(ST24)、既に行使されている場合にはログインは拒否される(ST25)。

【0041】次に、チケットデータ生成部32dにより、転送されたクライアントパラメータPを上述した一方関数で要約した第2のチケットデータD2を作成し、第1のチケットデータD1とを照合し(ST26)、不一致の場合にはログインは拒否される(ST27)。

【0042】次に、IDが既に登録されているものか否かを検索し(ST28)、登録されていれば後述するST30に進み、登録されていなければIDが作成される(ST29)。そして、メインサーバ33へのログインが可能となる(ST30)。

【0043】なお、このようなアクセス認証システムの場合には、サービス提供先サービス提供者20からサービス提供元サービス提供者30にクライアントパラメータPが転送される際に、何らかの方法でクライアントパ

ラメータPを傍受し、クライアントパラメータPを改竄して不正アクセスしようとしても、第1のチケットデータD1と改竄されたクライアントパラメータPに基づいて作成された第2のチケットデータD2とが不一致となり、ログインが拒否されることになる。

【0044】なお、改竄されたクライアントパラメータPに基づいて第1のチケットデータD1を作成することにより、新たなサービス提供元サービス提供者30へのログインが可能になる。しかしながら、第1のチケットデータD1の作成には共通の文字列を知る必要がある。しかも、この共通の文字列は、認証サーバ22、32に侵入して入手したり、総当たり法によって推測したり、一方関数の逆演算して導き出すことが考えられるが、共通の文字列の更新を十分に短く設定することで、事実上共通の文字列を入手することが困難になる。

【0045】また、クライアントパラメータP及び第1のチケットデータD1を流用しようとしても、有効期限を十分に短く設定しておけば、有効期限後のアクセスとなる可能性が高く、ログインが拒否されることになる。

【0046】さらに、有効期限内の使用であっても、正規のユーザによるサービス提供元サービス提供者30へのアクセスとはほぼ同時である。このため、クライアントパラメータP及び第1のチケットデータD1を第三者が傍受し不正使用しようとしても、既に正規のユーザによって第1のチケットデータD1の行使が済んでおり、第三者の第1のチケットデータD1ではログインができない。

【0047】一方、正規なユーザが共通の文字列を含んだ状態で生成された第1のチケットデータD1をサービス提供元サービス提供者30に到達した時点で、共通の文字列が更新されていて第2のチケットデータD2と第1のチケットデータD1が異なってしまうログインが拒絶されてしまう問題は、次のようにして解決する。

【0048】例えば、定期的にA、B、C、Dという順番で共通の文字列を変える場合、AB、BC、CD、…というように2つの共通の文字列を組み合わせることで、2種類の第1のチケットデータD1を作成し、この2つの第1のチケットデータD1のいずれかが第2のチケットデータD2と一致すればログイン可能とするように設定することにより対処する。

【0049】上述したように、本発明の一実施の形態に係るアクセス認証システムによれば、クライアントは、1つのサービス提供先サービス提供者に対してのID及びパスワードのみで、各種サービスを提供する他のサービス提供元サービス提供者にパスワードを開示することなく利用することが可能となる。また、サービス提供先サービス提供者からサービス提供元サービス提供者に転送されるデータが第三者により傍受された場合であっても、何重にも安全対策が講じられているため、サービス

10

20

30

40

50



提供元サービス提供者に不正にアクセスがされることがない。

【0050】なお、上述したシステムは、各サーバ等のコンピュータにインストールされたプログラムの指示に基づき実行されるものであってもよく、また、プログラムの指示に基づきコンピュータ上で稼動しているオペレーティングシステム、ミドルウェア等が各処理の一部を実行するようにしてもよい。

【0051】また、プログラムは、コンピュータが読取可能な記憶媒体に格納された状態で提供されるようにしてもよい。例えば、記憶媒体としては、磁気ディスク、フロッピー（登録商標）ディスク、ハードディスク、光ディスク（CD-ROM、CD-R、DVD等）、MO、半導体メモリ等のようにプログラムを記憶でき、コンピュータが読取可能であるようなものであればよい。

【0052】さらに、プログラムは、LANやインターネット等により伝送されるようにしたものでもよい。

【0053】なお、本発明は前記実施の形態に限定されるものではなく、本発明の要旨を逸脱しない範囲で種々変形実施可能であるのは勿論である。

\*20

\*【0054】

【発明の効果】本発明によれば、クライアントは、1つのサーバ（サービス提供者）に対しての個人情報（ID及びパスワード）のみで、各種サービスを提供する他のサーバ（サービス提供者）を個人情報の全てを開示することなく利用することが可能となる。

【図面の簡単な説明】

【図1】本発明の一実施の形態に係るアクセス認証システムの構成を示す図。

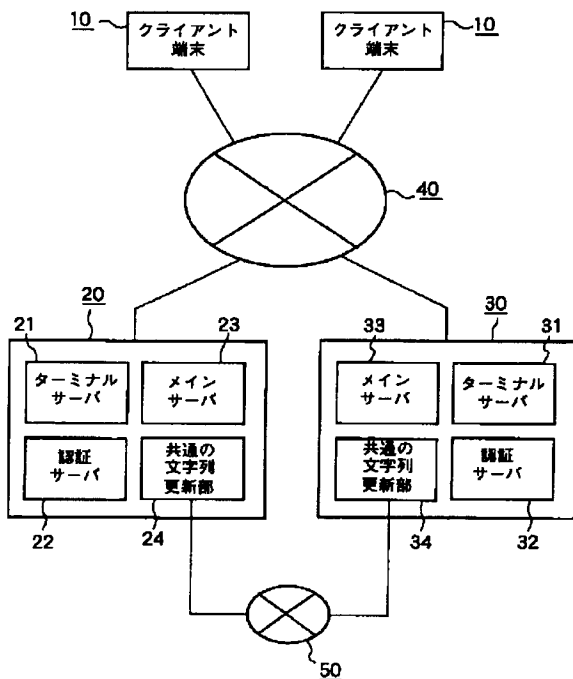
10…クライアント端末  
20…サービス提供先サービス提供者  
30…サービス提供元サービス提供者  
40…インターネット回線  
50…電話回線

【図2】同アクセス認証システムの動作を示すフロー図。

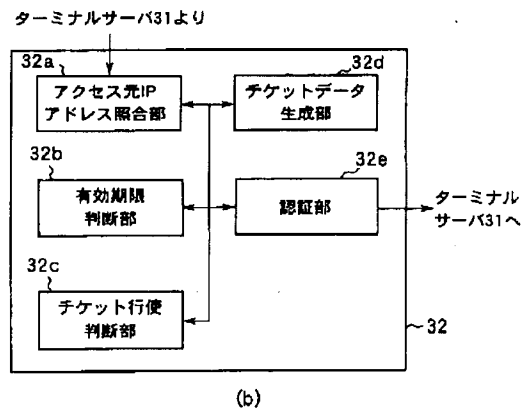
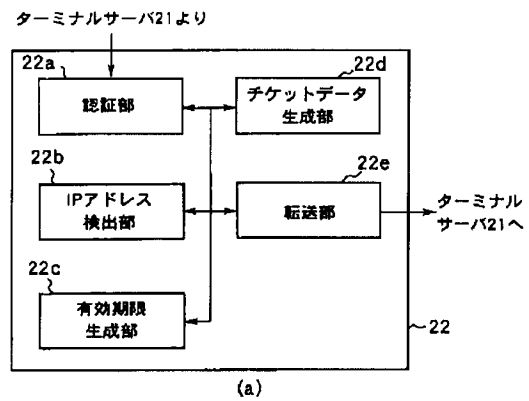
【符号の説明】

- 10…クライアント端末
- 20…サービス提供先サービス提供者
- 30…サービス提供元サービス提供者
- 40…インターネット回線
- 50…電話回線

【図1】



【図2】



【図3】

